



## Evolving SVG

Linda Cornwall, STFC, UKRI

GridPP meeting 25<sup>th</sup> April 2019

---

 [eosc-hub.eu](https://eosc-hub.eu)

 [@EOSC\\_eu](https://twitter.com/EOSC_eu)

**Dissemination level:** Public/Confidential *If confidential, please define:*

Disclosing Party: (those disclosing confidential information)

Recipient Party: (to whom this information is disclosed, default: project consortium)



- SVG = Software Vulnerability Group
- Main Purpose – to prevent Security Incidents due to software vulnerabilities
  - In EGI
  - But NOT trying to substitute/compete with various other vulnerability activities
- Advisories issued to sites for vulnerabilities which are
  - Relevant and serious and/or
  - In software which has been developed to enable the shared infrastructure
- Been running in current form since 2005 with relatively minor changes including
  - Going from being focussed on Grid Middleware to all types of software on the EGI distributed infrastructure
  - Encompassing EGI FedCloud

- Proliferation of software and technology has occurred
  - The distributed infrastructure is less and less homogenous as time goes on
- Now including services in the EOSC-hub Catalogue
- Software Vulnerability Group (SVG) Risk Assessment Team (RAT) cannot be experts in all software, services and configuration
  - Nor can they be looking out for advisories on all software that may be used
- Need a new approach
  - SVG has to hook into the evolving world the best way we can

- Confluence exploited

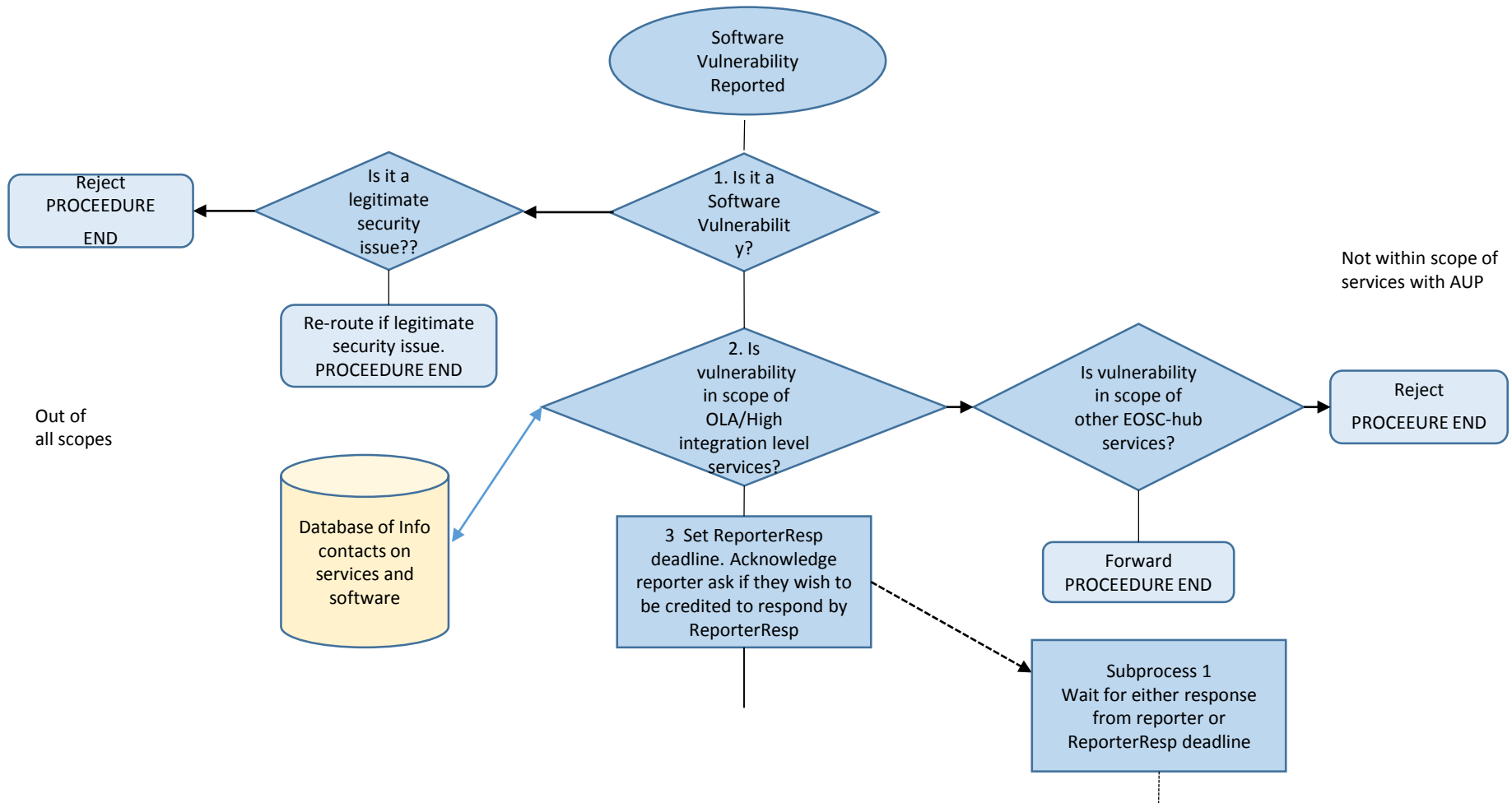
<https://www.egi.eu/security-announcement-10-april/>

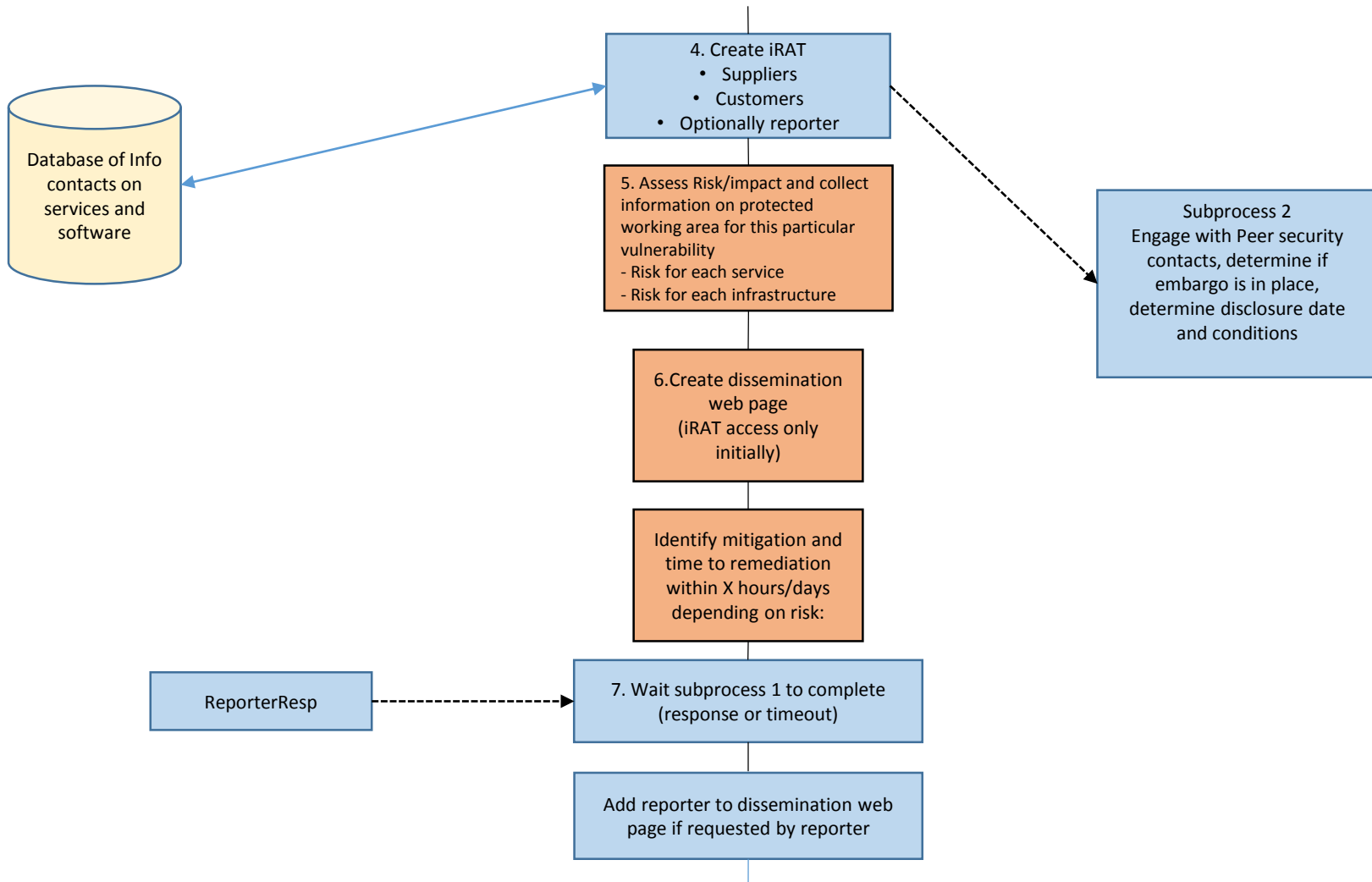
- The office systems were not considered in scope of SVG
- Critical advisory on confluence had been made public on 20<sup>th</sup> March

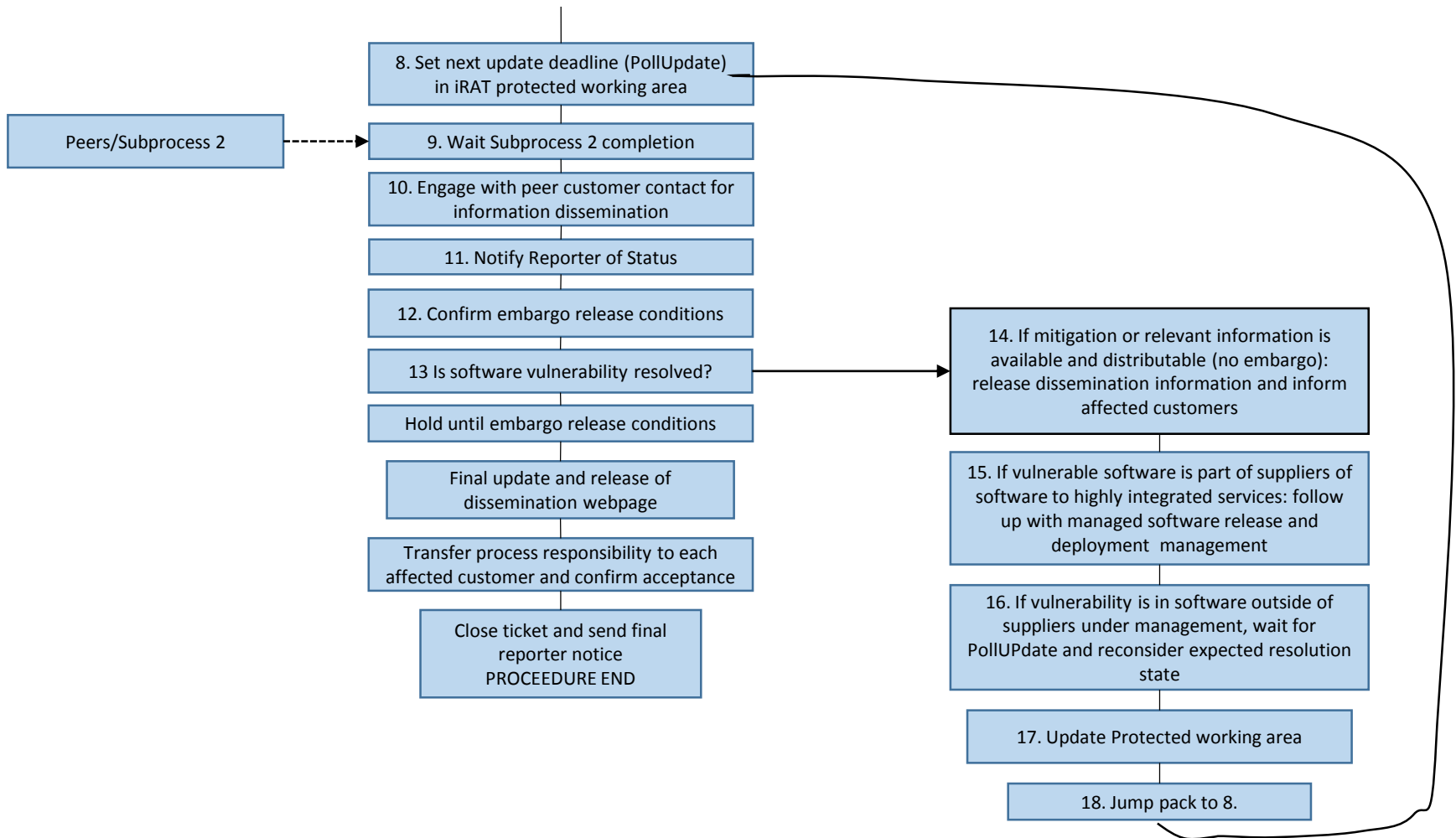
<https://confluence.atlassian.com/doc/confluence-security-advisory-2019-03-20-966660264.html>

- Yet exploit happened on 10<sup>th</sup> April
- If confluence had been patched quickly...

- Need to depend on experts on software and services to assess a vulnerability
- When a new software vulnerability is reported:-
  - Need to be able to contact the appropriate experts easily
    - Software developers
    - Those who set up services which depend on the software
  - Then set up an Issue Risk Assessment Team (iRAT) to handle this vulnerability
- Devised a new procedure – first in April 2018, then revised in November 2018
  - Put into FitSM format (EOSC-hub using this)
  - And a diagram







- We have identified a fair number of tools and sub-procedures to make this work
- But, the most important ones are determining Scope and forming the iRAT.

- Working out whether issue is in scope
- Scope defined as "Any software used to enable 'High level Integration' services".
  - For now
- It includes EGI UMD/CMD
  - These used by services, AND EGI endorses them
- Probably should include the various office services
  - And get experts involved who run such services

- Concept of the iRAT – or Issue Risk Assessment Team is the biggest change in the SVG evolution
- After appropriate experts have been contacted the iRAT is formed which
  - Investigates the vulnerability, and the effect of the vulnerability on the various services
  - Assesses the risk to those services.
  - Works out how to mitigate the problem, whether update software with a patch or carry out other action
  - Drafts appropriate notification/advisory
- Then notification/advisory is sent to the relevant parties defining what actions should be carried out.

- How to determine scope and form the iRAT?
- For EGI UMD/CMD software – simple to contact the right people
- For the services, the difficult bits are how to find who to contact and what services are using what software
- Ideally a database of software and contacts/experts used in all services in EOSC-hub service catalogue
  - But we don't have it
- To start, we could consider service contacts/security contacts from definitive list of services
  - Except that's not there yet either
- Hoping to start with access to a definitive service list, which EOSC-hub is developing

- A long way to go!

# Thank you for your attention!

---

*Questions?*



## EOOSC-hub

 [eosc-hub.eu](https://eosc-hub.eu)  [@EOOSC\\_eu](https://twitter.com/EOSC_eu)



This material by Parties of the EOOSC-hub Consortium is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

- SVG has been handling vulnerabilities since 2005
  - Handling vulnerabilities which affect the EGI infrastructure and its predecessors
  - To help prevent security incidents
- Anyone may report an issue by e-mail to [report-vulnerability@egi.eu](mailto:report-vulnerability@egi.eu)
- If it has not been announced, SVG contacts the software provider and the software provider investigates (with SVG member, reporter, others)
- If relevant to EGI the risk in the EGI environment is assessed, and put in 1 of 4 categories – ‘Critical’, ‘High’, ‘Moderate’ or ‘Low’
- If it has not been fixed, Target Date (TD) for resolution is set - ‘High’ 6 weeks, ‘Moderate’ 4 months, ‘Low’ 1 year
- Advisory is issued by SVG
  - If the issue is ‘Critical’ or ‘High’ in the EGI infrastructure
  - When the vulnerability is fixed if EGI SVG is the main handler of vulnerabilities for this software, or software is in EGI Repository regardless of the risk.
  - If we think there is a good reason to issue an advisory to the sites.
- Critical vulnerabilities are handled with top priority, aiming for a resolution within 1 day
- <https://documents.egi.eu/public/ShowDocument?docid=3145>